



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/679,333	10/04/2000	Stefan Hepper	DE919990073US1	6558
46369	7590	03/27/2006	EXAMINER	
HESLIN ROTHENBERG FARLEY & MESITI P.C. 5 COLUMBIA CIRCLE ALBANY, NY 12203			LANIER, BENJAMIN E	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 03/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/679,333	HEPPER ET AL.
	Examiner	Art Unit
	Benjamin E Lanier	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 27 February 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-17, 19 and 20 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-17, 19 and 20 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 04 October 2000 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 27 February 2006 amends claims 1, 3, 17, and 20.

Applicant's amendment has been fully considered and is entered. The amendments to claims 1 and 3 have overcome the previous §112 second paragraph rejections.

Response to Arguments

2. Applicant's arguments filed 27 February 2006 have been fully considered but they are not persuasive. Applicant's argument that Peyret does not teach or suggest any processing protocol between the server and terminal which would reduce data transfers between the server and the client is not persuasive because the claim limitation merely suggests that the act of transmitting the signed, and bundled command sequence as a data packet to the client results in reduced data transfers between the server and the client. Therefore, because the prior art teaches the transmission limitation, the result would be the same.

3. Applicant's argument that Peyret does not disclose the concept of bundling is not persuasive because Peyret discloses that the server generates the applets for a smart card (Col. 5, lines 36-38). This meets the limitation of bundling commands to produce a bundle command sequence because an applet is made up of many commands, and the applet generation processing would comprise the "bundling" of these commands into a single application or applet. The term "bundling" is extremely broad and has been given a broad but reasonable interpretation as applied to the Peyret reference.

4. Applicant's notion that the applets of Peyret are pre-complied is not persuasive because Peyret discloses that the applets are generated for the smart cards (Col. 5, lines 36-38). Pre-compilation would not be consistent with this teaching.

5. Applicant's argument that the current 103 rejections are no longer applicable because the independent claims have been amended to specify that the smart card is a processor-based smart card is not persuasive because the smart card in the Peyret reference contains a processor (Abstract). The fact that the Chen reference discloses a memory card and not a processor-based smart card is irrelevant, because the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). One of ordinary skill in the art would have been motivated to unpack the application program of Peyret on the user terminal before transferring the application to the smart card in order to minimize the decisions required of a user when installing an application as taught in Chen (Col. 9, lines 24-26).

6. Applicant's argument that the Chen reference is non-analogous because the portable computer itself performs the unpacking and not the client is not persuasive because the portable computer of Chen would be considered the client within a client/servers system. The claim limitations require unpacking by the client (portable computer, desktop, etc.) and transmission of the unpacked commands to the smart card, which in the case of Chen would be the memory card.

Once again, the limitations of a processor-based smart card are fully disclosed in the primary reference (Peyret).

7. The Examiner is unsure why Applicant is comparing the personal computer of Chen to the smart card of Peyret because they are not being relied upon to read on the same object in the claim limitations. The personal computer of Chen would be equivalent to the terminal (Figure 4, element 80), and would read on the client from the claim limitations. The smart card of Peyret would be equivalent to the memory card of Chen, and would read on the smart card from the claim limitations. Therefore, Applicant's analysis on page 16 does not take into account the combination of the references.

8. Applicant's argument that there would be no need to unpack an applet in an intermediary structure prior to receipt by a smart card is not persuasive because smart card memories be small in comparison to computer system memories, and would therefore benefit from having only to process individual instructions/commands transmitted from the client computer.

9. With respect to Applicant's argument that an applet cannot be unpacked, an applet is simply an executable file, and when executables are run, they individual computer instructions/commands are "unpacked" for execution. An applet, or any other executable, cannot be processed as a whole but are processed instruction by instruction.

10. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the

Art Unit: 2132

applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. Claims 1, 4, 6, 8, 11-15, 17, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of Zumkehr, U.S. Patent No. 5,974,529. Referring to claims 1, 4, 6, 12-15, 17, 20, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the authenticity of the terminal and of the server and visa versa, which meets the limitation of a processor-based smart card. If the server and the smart

card authenticate each other, then the loader within the smart card begins the loading process (Col. 7; lines 42-67). Once an application is selected to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53), which meets the limitation of sending a request from the client to the server for a smart card application component. Peyret discloses that the smart card receives applets from the server and that these applets can be used to download new versions of the applets (Col. 8, lines 27-37), which meets the limitation of bundling in the server a sequence of commands to produce a bundled command sequence for downloading of the application component to the smart card. Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the bundled command sequence, transmission of the signed command sequence as a data packet to the client. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature and execution of the commands on the smart card and execution of the commands on the smart card if the digital signature is correct. Peyret does not disclose that the application is unpacked at the user terminal before being installed on the smart card. Chen discloses a method for installing an application wherein a desktop manager on the user terminal unpacks the application program before installing the program on the memory card (Col. 8, line 66 – Col. 9, line 22), which meets the limitation of unpacking of the data packet by the client and transmission of the individual commands of the bundled command sequence in sequence to the smart card. It would have been obvious to one of ordinary skill in the art at the time the invention was made to unpack the application program of Peyret on the user terminal before transferring

the application to the smart card in order to minimize the decisions required of a user when installing an application as taught in Chen (Col. 9, lines 24-26). Peyret does not disclose that each individual instruction of the application is digital signed. Zumkehr discloses a system for error detection wherein individual program instructions are digitally signed and later authenticated (Col. 2, lines 29-47). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the application instructions of Peyret to be digitally signed in order to provide low detection latency as taught in Zumkehr (Col. 2, lines 47-50). Applicant's argument that Peyret does not teach or suggest any processing protocol between the server and terminal which would reduce data transfers between the server and the client is not persuasive because the claim limitation merely suggests that the act of transmitting the signed, and bundled command sequence as a data packet to the client results in reduced data transfers between the server and the client. Therefore, because the prior art teaches the transmission limitation, the result would be the same.

Referring to claim 8, Peyret discloses that the cryptosystem used can be a public key cryptosystem (asymmetrical) (Col. 5, lines 31-33).

Referring to claim 11, APDU protocol is the protocol used to communication with a smart card, which meets the limitation of the command sequence as a minimum comprises an Install command, one or more Load commands and a final Install command, and is stored in an APDU structure.

14. Claims 2, 7, 10, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of Zumkehr, U.S. Patent No. 5,974,529 as applied to claims 1-3, 17 above, and further in

view of Everett, U.S. Patent No. 6,575,372. Referring to claims 2, 7, 10, 19, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature and execution of the commands if the digital signature is correct. Chen discloses a method for installing an application wherein a desktop manager on the user terminal unpacks the application program before installing the program on the memory card (Col. 8, line 66 – Col. 9, line 22), which meets the limitation of unpacking of the data packet by the client and transmission of the individual commands in sequence to the smart card. Zumkehr discloses a system for error detection wherein individual program instructions are digitally signed and later authenticated (Col. 2, lines 29-47). Peyret does

not disclose that the keys are generated based on card identification data. Everett discloses an IC card loading system wherein to generate cryptographic keys for each individual IC card, a certificate authority uses card identification information transmitted from the terminal in order to generate individual key sets for the IC cards (Col. 5, lines 42-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the cryptographic keys of Peyret to be generated based on the IC card identification data in order to easily identify and authenticate the cards at a later point in time as taught in Everett (Col. 8, lines 25-34).

15. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of Zumkehr, U.S. Patent No. 5,974,529 as applied to claims 1, 13 above, and further in view of Hanel, GB 2,314,948. Referring to claim 16, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session

key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature and execution of the commands if the digital signature is correct. Chen discloses a method for installing an application wherein a desktop manager on the user terminal unpacks the application program before installing the program on the memory card (Col. 8, line 66 – Col. 9, line 22), which meets the limitation of unpacking of the data packet by the client and transmission of the individual commands in sequence to the smart card. Zumkehr discloses a system for error detection wherein individual program instructions are digitally signed and later authenticated (Col. 2, lines 29-47). Peyret does not disclose using message authentication codes in the command codes. Hanel discloses a chipcard data transfer method wherein message authentication codes are appended to commands (Page 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the commands of Peyret to include a MAC because it is a known procedure as disclosed in Hanel (Page 1).

16. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of Zumkehr, U.S. Patent No. 5,974,529 as applied to claim 1 above, and further in view of Klingman, U.S. Patent No. 5,729,594. Referring to claim 5, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the

authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature and execution of the commands if the digital signature is correct. Chen discloses a method for installing an application wherein a desktop manager on the user terminal unpacks the application program before installing the program on the memory card (Col. 8, line 66 – Col. 9, line 22), which meets the limitation of unpacking of the data packet by the client and transmission of the individual commands in sequence to the smart card. Zumkehr discloses a system for error detection wherein individual program instructions are digitally signed and later authenticated (Col. 2, lines 29-47). Peyret does not disclose communication using SSL. Klingman discloses client server communications using SSL (Col. 3, lines 32-36). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use SSL in the communications of Peyret in order to provide a secure communication line as taught in Klingman (Col. 3, lines 37-39).

17. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Chen, U.S. Patent No. 6,360,364, and further in view of Zumkehr, U.S. Patent No. 5,974,529 as applied to claims 1, 8 above, and further in view of Schneier. Referring to claim 9, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature and execution of the commands if the digital signature is correct. Chen discloses a method for installing an application wherein a desktop manager on the user terminal unpacks the application program before installing the program on the memory card (Col. 8, line 66 – Col. 9, line 22), which meets the limitation of unpacking of the data packet by the client and transmission of the

individual commands in sequence to the smart card. Zumkehr discloses a system for error detection wherein individual program instructions are digitally signed and later authenticated (Col. 2, lines 29-47). Peyret discloses the use of public key cryptography but does not disclose the use of RSA. Schneier discloses that RSA is a form of public key cryptography (Page 366). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use RSA as the public key cryptographic method in Peyret because RSA is the most popular form of public key cryptography as disclosed in Schneier (Page 366-367).

Allowable Subject Matter

18. Claim 3 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

19. The following is a statement of reasons for the indication of allowable subject matter: The prior art does not disclose or make obvious a method of generating a session key that is used for digitally signing individual commands for a smart card, and an authentication method wherein a server generates a first random number and transmits the random number to a client that provides an interface for a smart card. The client transmits the first random number to the smart card, and the smart card generates a session key using the first random number and a second random number generated at the smart card. The smart card then encrypts the first and second random number for transmission, along with the unencrypted second random number, back to the server via the client computer, where the server also generates the session key using the first and second random numbers and authenticates the transmission by decrypting the encrypted random numbers and comparing.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



Gilberto Barron Jr.
GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100